Commonwealth Office of Technology

Security Awareness Newsletter

Published by the COT Division of Security Services

October 2004 Volume 11, Issue 4

Inside this issue:

October's Security Tip

Home Computer Installation

STOP! Before you connect your new home computer to the Internet, follow these steps, especially if you plan to use the PC to connect to the state's networks.

—Install a hardware-based firewall, if possible. Many cable/DSL modems have this feature built in.

—Install a software firewall such as BlackIce or Zone Alarm or enable the operating system's firewall, if available.

—Install virus protection software.

—Disable file and print sharing services.

—Once you've performed these steps, you will be fairly well protected to connect to the Internet. At this point, you should download and install software patches.

For more info, visit the CERT Coordination Ctr.

Tips for Creating Policy Compliant Passwords

The majority of the Commonwealth's information systems rely upon userID/password authentication to provide secure system access for its users. Passwords, particularly those with administrative privileges, function as 'gateways' to systems that if compromised, could allow intruders access into the Commonwealth's networks. For that reason, it is crucial that employees understand and observe the password policies in place at both the agency and enterprise levels.

Creating strong passwords that comply with security policies can often be a frustrating task. Ideally, passwords should be functionally strong, yet easy to use. They should be easy to remember, yet difficult to guess. Fulfilling these conditions, however, is not as easy as it sounds. Recent internal password audits conducted by COT show that a substantial percentage of employees' passwords do not comply with the Commonwealth's Enterprise UserID and Password Policy (CIO-072), which specifies the minimum password composition requirements. The majority of failing passwords violated one or more of the following enterprise password policy requirements:

- Passwords must be changed every 31 days, unless otherwise approved.
- Passwords may never be reused or shared with other people/userIDs.
- Passwords must be at least 8 characters long. Passwords for userIDs with privileged access must be at least 11 characters long. Note: Mainframe passwords for RACF userIDs must be 8 characters exactly—no more, no less.
- Passwords must ***not*** be sequences of letters or numbers.
- Passwords must ***not*** contain a word found in an English or foreign language dictionary, slang, names, persons, places, or things.
- Passwords must ***not*** be the same as the userID or things easily identifiable with the user.
- Passwords must ***not*** be vendor supplied default passwords or commonly used defaults.
- Passwords must ***not*** be blank or missing.
- Passwords must use a combination of upper and lower case letters, and must also contain a number.

It should be noted that the above list is not a complete summary of the Enterprise UserID and Password Policy or listing of its requirements. *Continued on page 2.*

Did You Know . . . The list below shows estimates for the time it takes password cracking software to reveal passwords based on their composition. *Note: Time estimates are for passwords that do not use dictionary words, since these type of passwords are easily cracked regardless of their length or composition.*

Password with 5 characters ····· seconds
Password with 8 characters (lower or upper case letters) ····· minutes
Password with 8 characters (lower & upper case letters) ····· 1 hour
Password with 8 characters (lower & upper case letters and number) ····· 12 hours
Password with 8 characters (lower & upper case letters, number AND a special character) ···· 2.5 months

Password Tips continued

Ideally, passwords should be completely random and composed of letters, numbers, and special characters (*, &, #, @, %, ~, !, ^, ", ?, <, >, etc.). (*Note: Mainframe RACF passwords only allow the use of the following special characters — @, #, $*).

How easy is that to remember? Not very! By the time you have memorized your old password, the system will prompt you to create a new one. So the question remains, "How can a user create a complex, policy-compliant password that is easy to remember?" The most common method utilized by the IT industry makes use of pass phrases and substitution. Two such methods are explained in the following articles:

Microsoft Article—Creating Stronger Passwords
Kentucky Auditor Web Site—Characteristics and Suggestions for Stronger Passwords

Now, here is an idea! Since the Commonwealth's enterprise policy has a few requirements, why not try to create a random password based on that. For example, an uppercase letter, a lowercase letter, and a number. If you can come up with a way of selecting two of each, you will have 6 of the 8 required characters. For the remaining two, you could use special characters such as a '?' or '$'.

You may also want to use the techniques discussed in the articles above to make your password selection. For example:

- "The cow jumped over the moon." This is a phrase that most everyone is familiar with so why not use the first letters of the first four words to select the upper and lower cases letters required for your password — **T C j o**.

- Now for two numbers. Try not to select numbers such as the current month and year. Base your selection on something you can easily remember. For example, maybe your favorite condiment is ketchup and this makes you think of Heinz 57 Varieties. Now an easily remembered password is beginning to take form — **T C j o 5 7**.

- Don't forget about special characters. As mentioned earlier in this article, special characters are recommended but not required by policy; however, using a special character makes it more difficult for someone to crack your password. Since you have a vivid picture in your mind now of a cow jumping over the moon with a bottle of ketchup, all you have left is to select two random special characters such as '@' *and '(*'. Now your password is complete—**T C j o 5 7 @ (**.

After typing this password in at logon a few times, it should become easier to remember. Stay tuned for future articles that will explore other password creation techniques to help users create secure, policy-compliant passwords.

Contributor/Writer—Joe Rach, COT Security Engineer

To give employees a better understanding of why the Commonwealth requires such complex composition rules for passwords, listed below are some common steps hackers/crackers use to uncover system passwords:

Step 1—The first password guess a cracker usually tries is the userID, since many users often use their userID as a password.
Step 2—The next try is the user's name. Passwords based on userIDs or names are common and are a cinch for hackers to guess.
Step 3—Does the password use a common dictionary word or name? A hacker will use dictionary and name lists to crack this type of password in 30 minutes to 6 hours.
Step 4—Does the password use a foreign name or phrase? It takes a hacker 18 hours to crack this type of password.
Step 5—If the password has not been revealed at this point, the hacker will perform a brute force attack in which every possible combination of letters, numbers, and characters are used until the password is discovered. This could take the hacker weeks or even months to crack a complex, policy-compliant password. But keep in mind, automated software cracking tools are constantly improving, greatly reducing the time it takes to crack even the most complex passwords.

Advisory—Microsoft Outlook Meeting Request

Outlook's calendar function is a great tool for wading through hectic schedules to organize meetings. Users should be aware, however, that any documents attached to an Outlook meeting request are accessible not only to the meeting invitees, but to anyone who has rights to view the organizer's or meeting participant's calendar.

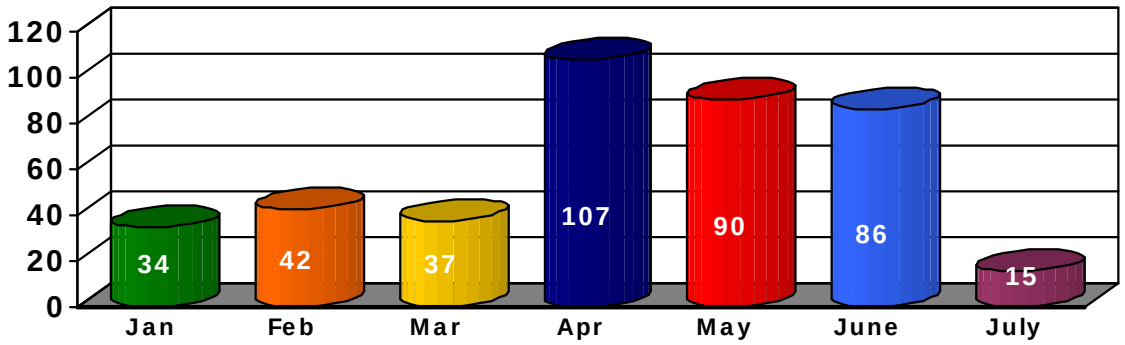
If you need to distribute sensitive documents to attendees, COT recommends that these be sent in a separate email. Or another option is to select the PRIVATE checkbox found at the lower right of the meeting request window. This option not only prevents meeting attachments from being read by those not invited to the meeting, it also keeps details confidential such as the attendees' names, meeting purpose, and any messages included in the meeting request.

Note: COT employees are encouraged to setup their Outlook calendars to allow the COT ALL distribution list 'reviewer' permissions. Reviewer access allows your calendar to be viewed (but not edited) by all COT employees and contractors, making it easier for meeting organizers to setup meetings. For assistance with changing your calendar's permissions, contact your LAN support technician.

McAfee Agreement Update

McAfee is currently the Commonwealth's enterprise standard for virus protection. In 2003, COT announced a new licensing agreement between the Commonwealth of Kentucky and McAfee (formerly Network Associates, Inc.) for its anti-virus products. The 2003 agreement afforded agencies the ability to work directly with McAfee (as opposed to COT) to purchase software licenses and support. Some changes have recently been made to the agreement that will make it a better value for the Commonwealth. COT will distribute an agency contact memo as soon as details are confirmed. Procurements will be processed by authorized resellers, Software Spectrum and Zones, Inc.

COT Monthly Incident Report Totals* for Malicious Code
January—July 2004



*The numbers reflected in the chart are based on voluntary reports of security incidents submitted by COT employees and other state agencies. The actual incidence of malicious code may be higher.

Did You Know . . . The most common signs of malicious code infection are:

— Applications function abnormally.
— Disks become inaccessible.
— Experience printing difficulties.
— Pull-down menus appear distorted.
— File sizes change.
— Unusual error messages.
— Last access date of files does not match with actual time file was last used.
— Increased number of files on a system (although no additional files have been added).
— Disk light shows activity when there should be none.
— Computer is slow, freezes up, or crashes.

XP Service Pack 2 Implementation

In August 2004, COT released an advisory requesting that state agencies with computers running Microsoft XP update them with Service Pack 2 (SP2) by November 1, 2004. Updating to SP2 will also protect machines from the widely publicized Download.Ject vulnerability that can compromise systems running XP SP1 or lower. SP2, XP's first major security fix, provides the following enhanced security features:

—Default activation of Windows Firewall upon installation.
—More secure Web browsing due to a restricted ActiveX configuration.
—Consolidated security features (Windows Security Center), making it easier for administrators to keep track of security settings.

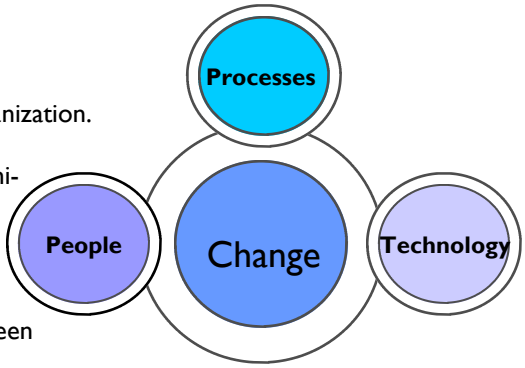
While applying the XP SP2 update provides additional security, it can also cause problems with many security and firewall utility software and may result in some custom-built software incompatibilities. Conflicts with existing firewall products such as BlackIce may occur. In addition, it is possible that SP2 may cause some Web sites from functioning properly due to new security-related dialog boxes. To prevent such problems, COT recommends agencies begin testing SP2 as soon as possible and develop a plan for implementation no earlier than October 1, 2004 to allow time for initial problems to be identified and resolved.

For more information on XP's Service Pack 2 and COT's recommendations for testing and implementation, reference the August 24, 2004 Enterprise Architecture Advisory.

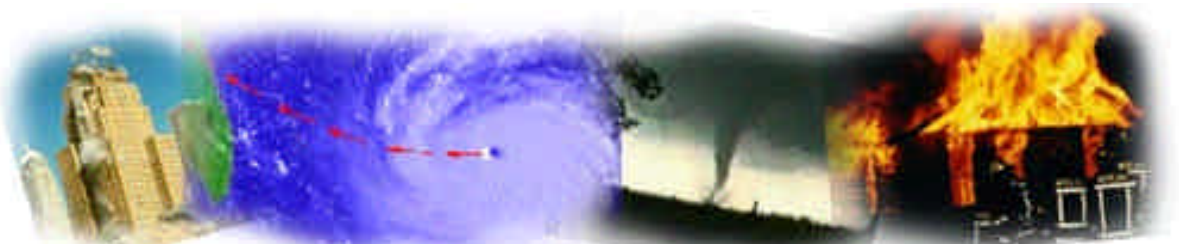
The COT IT Change Management/Control Process

IT Change Management/Control can be defined as a process for improving the management of changes to the computer and networking infrastructure. The Commonwealth Office of Technology manages and maintains numerous mission critical information systems that provide vital services to Kentuckians. In order to prevent unnecessary service disruption arising from change-related incidents, a change management/control process was established to ensure that any and all changes, updates, or modifications to the COT-managed IT environment are properly approved, communicated and implemented on a timely basis. Listed below are some of the types of changes that should be included in the change management process:

— Periodic maintenance.
— User requests of changes or moves/updates.
— Hardware, software, application and/or database upgrades & reorganization.
— Acquisition of new hardware and/or software.
— Changes or modifications to the infrastructure and all data communication networks.
— Environmental changes.
— Operations schedule changes.
— Changes in hours of availability.
— All types of security requests, emergency requests and any unforeseen events.



Please note that the above list is not all inclusive. If you are not sure that a change request needs to be completed, contact COT's Buck Beverly. If you have a system that is managed by COT and you would like to submit a change control request, you can do so online by visiting the COT Change Management Web Site. You must acquire appropriate management approval before submitting the request. All change requests must be submitted by 10:00 a.m. Wednesday in order for the request to be included in the week's schedule. Change requests can be submitted up to three months in advance of the change. *Important Note: The change control process applies to all system changes and should not be replaced by other modes of communications, i.e. agency contact memoranda.* If you would like to learn more about COT's Change Management Policy, click on this link.



Planning for a Disaster—Alternative Recovery Sites

Did you know that according to research conducted by Coopers & Lybrand of companies that will experience a disaster and do not have a Disaster Recovery Plan (DRP) in place:

40 percent will face outright collapse.
40 percent will fail within 18 months.
12 percent will fail within 5 years.
Only 8 percent will survive the long term.

Agencies need to realize the impact the citizens of the Commonwealth will face with the loss of services. In the event of a disaster, there needs to be assurance that critical systems and data can be recovered within a reasonable time frame for our citizens.

If the Commonwealth Data Center (CDC) is not available, what facilities do we use? Where do we go? Where do we get needed equipment? What procedures are in place to ensure recovery? These questions can be answered with a current DR Plan in place that includes a recovery site.

One type of recovery site is known as a 'Hot Site,' which is an alternate facility that can become 'hot' or activated to be used in the event of an emergency. This type of site is fully equipped and operational with all of the necessary hardware to prepare for these events. Basically, with a hot site you can quickly relocate your critical business functions to an alternate facility with all the requirements and equipment in place to restore your IT processes if a disaster hits the main data facility, ensuring as brief as possible down time.

Often times companies contract for not only a recovery Hot Site, but also a Cold Site. A Cold Site is an empty space that has wiring and power that an organization can use in the event of a disaster. The organization must then provide all of the hardware and equipment necessary for the recovery process, making it a less expensive solution. However, during a down time of critical data or systems that need to be up and running, a Cold Site takes much longer to recover than a Hot Site.

In the article, "The US Hot Site Market Analysis & Forecast," written by Tari Schreider of Contingency Planning Research, Schreider describes how the Hot Site industry has successfully recovered 582 companies between 1982 and 1998 with an average of 40 per year. The top reasons cited for the Hot Site relocations include loss of power, followed by hardware errors and then fires.

For an organization to successfully relocate to an off-site recovery location during a disaster, it is necessary to have scheduled tests. Disaster recovery services, such as scheduled testing at the recovery locations, should also be included in the services contract. Scheduled testing will help to ensure a smooth transition to the recovery site. The testing periods allow for disaster recovery plans to be updated and/or corrected and any unforeseen problems fixed before an actual disaster occurs. Without adequate testing, severe errors could occur that hinder an organization's ability to recover and lengthen down time. With critical systems and applications that are mandatory, longer down times could adversely impact the citizens of the Commonwealth.

Written by Kristy Holliday, COT Disaster Recovery Team

Did You Know . . . The ten most common effects of a disaster are:

1. Loss of business/customers.
2. Loss of credibility/goodwill.
3. Cash flow problems.
4. Degradation of services to customers.
5. Inability to pay staff.
6. Loss of production
7. Loss of operation data.
8. Financial loss.
9. Loss of financial control.
10. Loss of customer account management.

CYBER BYTES

Current Security News & Information

COT to Host IT Security Events this Fall

National Cyber Security Day—October 29, 2004*

The National Cyber Security Alliance has been promoting semi-annual National Cyber Security Days since 2002, which are coordinated with daylight savings in April and October in the United States. COT will commemorate National Cyber Security Day on October 29, 2004, by hosting events in CDC's Training Rooms A & B. All COT employees and contractors are invited to attend. More information will be distributed soon. To learn more about National Cyber Security Days, visit the Stay Safe Online Web site.

International Computer Security Day—November 30, 2004

Once again, COT will continue its tradition of celebrating International Computer Security Day by sponsoring a security-related event for its employees and contractors. Plans for this year's event are still in the works but be sure and mark your calendar so you don't miss out on this once a year event. More information will be emailed to staff in early November. If you want to learn more about International Computer Security Day, visit their Web site.

**National Cyber Security Day is officially October 31, but since that date falls on a Sunday this year, COT will celebrate the event on Friday, October 29.*

FTC Supports Bounties for Spammers

An article by Jonathon Krim of the Washington Post, *Cash Bounties for Spammers Win Limited FTC Backing*, published on SecurityFocus.com reports that the Federal Trade Commission supports offering cash rewards to people who assist the agency with identifying spammers. A commission set up to study the issue recommended that rewards should range from $100,000 to $250,000 in order to be effective. Read more.

Microsoft Introduces New Line of Keyboards and Mice that Use Fingerprint Recognition Technology

Software giant Microsoft announced this month a new line of keyboards and mice that use fingerprint recognition technology to allow users to forego traditional system access via passwords. While the news may sound like a step in the right direction for IT security folks who constantly preach to users about the importance of creating complex passwords, Microsoft advises that these products only be used for convenience and does not recommended them for securing computers that contain sensitive data. For more info, visit the Microsoft Web site.

Congressional Committee Approves Measure to Make Spyware a Crime

Net piracy and spyware are being targeted by Congress. The House and Judiciary Committee voted to make it a criminal offense to place Internet spyware on computers. The Committee also approved the Piracy Deterrence and Education Act of 2004, which is now ready for debate in the House of Representatives. Read more about this topic in an article by David McGuire of the Washington Post.

Microsoft Updates

Microsoft has released the following security updates for its operating systems and other software products. COT recommends that agencies devise procedures to ensure the timely installation of hardware and software patches/updates, as well as the update of virus definition files (aka DATs). A comprehensive list of hardware and software security vulnerabilities affecting multiple platforms can be found on the COT Security Alerts Web page.

Microsoft Security Bulletin MS04-027

Vulnerability in WordPerfect Converter Could Allow Code Execution (884933)

Important—A remote code execution exists in the WordPerfect Converter that is provided as part of the affected software. If a user is logged on with administrative privileges, an attacker who has successfully exploited this vulnerability could take complete control of an affected system.

Microsoft Security Bulletin MS04-028

Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution (833987)

Critical—A buffer overrun vulnerability exists in the processing of JPEG image formats that could allow remote code execution on an affected system. If a user is logged on with administrative privileges, an attacker who has successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges would be at less risk than users who operate with administrative privileges.

Update—Configuration Error Discovered in XP Service Pack 2

Security Tracker recently reported a vulnerability in Microsoft's Windows XP SP2 that will allow remote users access to file and print sharing even though the Windows firewall is enabled. At the time this newsletter was published, Microsoft had not released a security update for this flaw. More information can be found at SecurityTracker.com.

Automatically Update Your Computer

Windows Update allows you to automatically update your computer's operating system, software, and hardware with the latest security patches. To learn more, visit the Windows Update Site and follow the prompts.

Security at Home

Microsoft offers a helpful site for those who have Windows-based home computers. The site provides tips for increasing home computer security; especially important for those who use their home computers to connect to the Commonwealth's networks to check email or access other applications. By securing your home PC with virus protection software, a personal firewall, and updated security patches, you also protect the state's networks from compromise from hackers, malicious code and other unsavory security threats. Visit the Microsoft Protect Your PC site, for pointers on making your home computing environment more secure.

Fight Spyware at Home

Visit this Microsoft site that provides information, tools and software for protecting your home PC from spyware and unauthorized adware.

Commonwealth Office of Technology

Division of Security Services

101 Cold Harbor Drive
Frankfort, KY 40601

Phone: 502.564.7680

Email:
COTSecurityServices@ky.gov

We're on the Web!
ky.gov/got/security/

The information contained in this newsletter is intended for internal use only.

The Commonwealth Office of Technology's Security Awareness Newsletter is published bi-monthly by the Division of Security Services. Its purpose is to provide security & IT professionals with timely information on cyber vulnerabilities, information security trends, malicious code info, and security policies & best practices.

About the Division of Security Services

The Division of Security Services' (DSS) primary role is to protect and ensure the confidentiality, integrity and availability of the Commonwealth's computing environment, which includes the Kentucky Information Highway (KIH), Commonwealth Data Center (CDC) and other key state computing facilities.

Security Services is also responsible for the development and maintenance of COT's Security Policies and Procedures Manual (SPPM), disaster recovery/business continuity plan, and Security Administrator Manuals (SAMs) that aid network administrators in securely configuring Windows NT, 2000, 2003, and Unix Solaris & AIX systems. DSS also provides mainframe RACF support, incident management, disaster recovery administration and a number of security awareness activities. If you would like to learn more about the services provided by DSS, visit our Web page at ky.gov/got/security.

For more information on IT security, check out the following Web sites!

Center for Internet Security
Not-for-profit site designed to assist businesses in assessing and reducing IT-related security risks.

Crypto-Gram Newsletter
Free monthly email newsletter from security expert Bruce Schneier. Site contains a link for subscribing to the newsletter, as well as back issues.

Forum of Incident Response and Security Teams (FIRST)
Site to exchange security incident information and coordinate response activities.

How Stuff Works - Security Technology
Interesting site for those who want information on how various security technologies actual work.

InfraGuard
FBI & NIPC information sharing site.

NY Office of Cyber Security & Critical Infrastructure Coordination
Contains daily updates on the latest alerts, news and information in the world of Internet security, privacy online, and viruses.

Security Magazine
Latest industry articles on security technologies.